ОСТОРОЖНО!
ТЕЛЕФОННЫЕ МОШЕННИКИ!
НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Проверяйте сомнительную информацию, прежде чем отправить деньги, если Вам сообщили что:

Родственник в беде

Вы выиграли приз

Банковская карта заблокирована

ОМВД России по г.Пыть-Ях тел: 02, (3463) 464714

Ваша карта заблокирована

КАК ЭТО ПРОИСХОДИТ

Абонент получает SMS-сообщение: «Ваша карта заблокирована!» или «Заявка на перевод денежных средств принята!» с просьбой перезвонить на указанный номер телефона.

Вы перезваниваете. Собеседник представляется технической службой либо службой безопасности банка (какого именно не уточняют) и просит срочно передать данные карты или же с помощью банкомата ввести якобы код разблокировки. Для этой цели вас просят подойти к ближайшему банкомату, войти в меню оплаты номеров мобильной связи и набрать ряд цифр.

Помните! Совершая операцию по разблокировке карты или же отмене перевода, на самом деле вы перечисляете все средства на чужой абонентский номер или счет карты.

ЧТО НУЖНО СДЕЛАТЬ

Будьте бдительны! Ни один банк не будет рассылать подобные сообщения, а тем более спрашивать реквизиты карты. Поэтому все сообщения и звонки с подобными предупреждениями всегда мошенничество.

SMS-просьба о помощи

КАК ЭТО ПРОИСХОДИТ

Абонент получает SMS-сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

ЧТО НУЖНО СДЕЛАТЬ

Помните сами и объясните пожилым людям, детям и подросткам, что на SMS-сообщения с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Вы выиграли приз

КАК ЭТО ПРОИСХОДИТ

Вам звонят и сообщают о крупном выигрыше или приходит SMS с таким же сообщением.

Вас просят посетить сайт и ознакомиться с условиями акции или же позвонить по указанному в SMS номеру телефона. Вам сообщают о том, что надо уплатить госпошлину, оформить документы и перечислить на счет своего мобильного телефона 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».

Либо сообщают, что, чтобы получить приз, вам необходимо в течение минуты дозвониться в организацию. Вам отвечает сотрудник «призового отдела» и объясняет, что в течение часа нужно подготовить карты экспресс-оплаты любого номинала на указанную им сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя. Затем сообщает номер, куда надо перезвонить.

Также, поясняет порядок действий для получения приза: с 10:00 до 20:00 такого-то числа необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Затем мошенник объясняет порядок активации карт: стереть защитный слой с карты, позвонить в «призовой отдел» и при переключении на оператора сообщить свои коды.

ЧТО НУЖНО СДЕЛАТЬ

Необходимо знать, что оформление документов на участие в таких лотереях никогда не проводится только по телефону или Интернету.

Если вы узнали о существовании лотереи только в момент выигрыша, вас пытаются обмануть.

Ваш родственник попал в беду

КАК ЭТО ПРОИСХОДИТ

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Он сообщает, что для решения вопроса необходима определенная денежная сумма которую следует передать посреднику или осуществить денежный перевод на абонентский номер или банковскую карту.

ЧТО НУЖНО СДЕЛАТЬ

Прервать разговор и перезвонить тому человеку,

ПАМЯТКА
о порядке действий сотрудника при общении с гражданами по профилактике преступлений

Сотрудник полиции при посещении адреса вручает памятку «Как не стать жертвой мошенников» при этом доводит до гражданина основные формы и методы преступления в сфере IT-технологий.

Разъясните гражданину, что на территории округа основные методы похищения денежных средств это:

1. 1. С использованием телефонии:

- Преступники представляются сотрудниками банков, предлагают защитить средства от несанкционированного списания под различными предлогами, либо аннулировать заявку на кредит или получения денежной компенсации, выясняют конфиденциальные сведения банковских карт потерпевших, одноразовые пароли и выводят деньги на подконтрольные счета;

2. В сети интернет:

- Размещение мошеннических объявлений о продаже товаров на сайтах бесплатных объявлений «Авито», «Юла», а также в социальных сетях «В

контакте», «Одноклассники», «Инстограмм» или в групповых чатах мессенджеров (Telegram, WhatsApp, Viber);
- Под предлогом оказания различных услуг (съем жилья, мелкий ремонт, доставка груза, интим услуги) при условии предоплаты, после чего добавляют потерпевшего в «черный список»;
- Получение многопроцентных выигрышей под предлогом инвестирования, при размещении денежных средств на инвестиционных, торгово-биржевых и игровых площадках.

При общении с гражданином, объясните:
1. Если Вам позвонили с банка и сказали, что Ваши финансы в опасности, не стесняйтесь, прекратите разговор, положите трубку и перезвоните на номер горячей линии банка, который указан на обратной стороне банковской карты. Ни при каких случаях не сообщайте звонящему личные сведения о себе и тем более сведения о Вашей банковской карте!
2. Запомните!!!! Легкий заработок по инвестированию Ваших денежных средств в Биржевых он-лайн компаниях - это ложь!
3. При покупке или продаже товара на торговых интернет-площадках «Авито, «Юла» не переводите задаток за товар, который не видели своими глазами. Не переходите по ссылкам, которые Вам выслал продавец. Ведите общение только на сайте и не переходите в другие мессенджеры «Viber», «WhatsApp», «Telegram»

РЕКОМЕНДАЦИИ
о правилах безопасного использования компьютерных технологий, расчетных банковских карт, социальных сетей

На территории Ханты-Мансийского автономного округа Югры, в том числе на территории г. Урай отмечается рост совершения мошеннических действий в отношении граждан под видом оказания различных услуг, в том числе в банковской сфере, посредством мобильной связи и сети «Интернет». Зачастую потерпевшие от преступных посягательств граждане не осведомлены о вновь появляющихся видах и способах мошенничеств, ввиду чего не способны в полной мере обезопасить себя от таковых посягательств.

С целью предупреждения преступных посягательств в отношении граждан, рассмотрим имеющиеся виды, способы мошеннических действий, а также способы избежать столкновения с мошенником.

Мошенничества, совершаемые с использованием мобильного телефона (звонки):

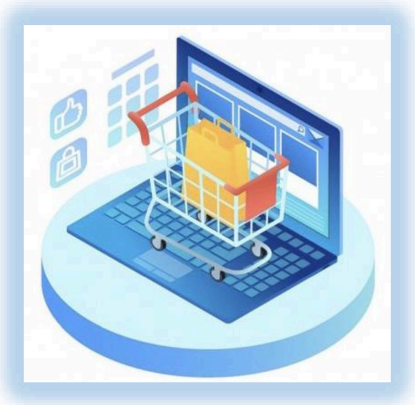
Социальные сети. В случае, если Ваш знакомый/близкий человек посредством сообщения в социальной сети просит Вас одолжить ему денежные средства (в долг), осуществите звонок данному человеку посредством сотовой связи и уточните, действительно ли именно Ваш знакомый/близкий человек просит Вас об одолжении. В СЛУЧАЕ, ЕСЛИ УКАЗАННЫЕ ДЕЙСТВИЯ ВАШ знакомый/близкий человек не осуществлял, НЕМЕДЛЕННО ПРЕКРАТИТЕ ДИАЛОГ С МОШЕННИКОМ И ОСУЩЕСТВИТЕ БЛОКИРОКУ КОНТАКТА от которого поступило сообщение с просьбой, так как вышеуказанные действия свидетельствуют о ВЗЛОМЕ СТРАНИЦЫ в социальной сети Вашего знакомого/близкого человека, ОБЯЗАТЕЛЬНО УВЕДОМИТЕ человека, чья страница была взломана.

НЕ РАЗМЕЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ, которыми могут воспользоваться МОШЕННИКИ!

Мошенничества, совершаемые с использованием сети «Интернет»

1. Звонок от сотрудника банка (сотрудника службы безопасности банка, финансового помощника): сотрудники финансово-кредитных организаций НЕ ОСУЩЕСТВЛЯЮТ ЗВОНКИ своим клиентам, а также НЕ ИНТЕРЕСУЮТСЯ ОБ ИМЕЮЩИХСЯ У НИХ БАНКОВСКИХ КАРТАХ, ДЕНЕЖНЫХ СРЕДСТВАХ, НЕ ТРЕБУЮТ НАЗВАТЬ КАКИЕ-ЛИБО РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ!

В случае, если Вам поступил звонок от неизвестного лица, которое сообщает Вам о том, что в отношении Вас совершаются мошеннические действия, на Вас оформили кредитное обязательство и иное, НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР, не нужно вести диалог с неизвестным лицом, если у Вас имеются сомнения по поводу сохранности Ваших денежных средств и их безопасности, обратитесь в отделение банка эмитента Вашей банковской карты или же осуществите звонок на горячую линию (абонентский номер указан с обратной стороны Вашей банковской карты) для получения подробной информации. НЕ СООБЩАЙТЕ РЕКВИЗИТЫ СВОЕЙ БАНКОСКОЙ КОД-ПАРОЛИ, ТРЕТЬИМ ЛИЦАМ!



2. Интернет сайты. НЕ ОСУЩЕСТВЛЯЙТЕ ЗАКАЗ ТОВАРОВ НА САЙТАХ, КОТОРЫМИ РАНЕЕ ВЫ НЕ ПОЛЬЗОВАЛИСЬ. В случае, если всё-таки возникла данная необходимость, прочтите отзывы о данном сайте.

При осуществлении покупок на сайте, который ранее Вы использовали, ОБРАТИТЕ ВНИМАНИЕ НА АДРЕСНУЮ СТРОКУ САЙТА (https://***), в случае, если В АДРЕСЕ САЙТА ПРИСУТСТВУЮТ ЛИШНИЕ СИМВОЛЫ, это свидетельствует о том, что ДАННЫЙ САЙТ ЯВЛЯЕТСЯ ДВОЙНИКОМ оригинального сайта, на котором ранее вы осуществляли покупки.
Пример:
https://www.tutu.ru/ (ОФИЦИАЛЬНЫЙ САЙТ);
https://www.tu-tul.com (САЙТ ДВОЙНИК - мошенник).

3. Мессенджеры. В случае, если Вам ПОСТУПИЛО СМС-УВЕДОМЛЕНИЕ в каком-либо МЕССЕНДЖЕРЕ ОТ НЕИЗВЕСТНОГО ОТПРАВИТЕЛЯ, содержащее в себе какую-либо ССЫЛКУ, НЕ ПЕРЕХОДИТЕ ПО УКАЗАННОЙ ССЫЛКЕ, ввиду того, что она может содержать вирусные угрозы (вирусы-мошенники). НЕ РЕАГИРУЙТЕ на поступающие смс-уведомления о ВЫИГРАШАХ, НЕОБХОДИМОСТИ ПОЛУЧЕНИЯ КАКИХ-ЛИБО ПОСОБИЙ и иное.
ВСЕ УКАЗАННЫЕ ДЕЙСТВИЯ СОВЕРШАЮТ МОШЕННИКИ!

4. Интернет платформы для продажи/покупки товаров. В случае, если Вы осуществляете покупку товаров посредством интернет платформ «АВИТО», «ЮЛА» и иных, НЕ ПЕРЕВОДИТЕ АВАНС ПРОДАВЦУ в счет оплаты товара. В СЛУЧАЕ, ЕСЛИ ПРОДАВЕЦ ВАС ТОРОПИТ С ПОКУПКОЙ/ОСУЩЕСТВЛЕНИЕМ ПЛАТЕЖА, это может свидетельствовать о том, что данный продавец – МОШЕННИК! НЕ ПРЕХОДИТЕ ПО ССЫЛКАМ, КОТОРЫЕ НАПРАВЛЯЕТ ВАМ ПРОДАВЕЦ под видом ссылки на переход для оплаты посредством сервиса быстрых платежей.
В случае, если Вы осуществляете продажу товара посредством интернет платформ «АВИТО», «ЮЛА» и иных, НЕ СООБЩАЙТЕ ПОКУПАТЕЛЮ БАНКОВСКИЕ РЕКВИЗИТЫ СВОЕЙ БАНКОВСКОЙ КАРТЫ для оплаты товара. НЕ ПРЕХОДИТЕ ПО ССЫЛКАМ, КОТОРЫЕ НАПРАВЛЯЕТ ВАМ ПОКУПАТЕЛЬ под видом ссылки на переход для оплаты посредством сервиса быстрых платежей.

Будьте бдительны к своим финансам и распространению персональных данных!

* СТАРАЙТЕСЬ ИЗБЕГАТЬ ПЛАТЕЖЕЙ В СЕТИ ИНТЕРНЕТ ПОСРЕДСТВОМ СВОЕЙ БАНКОВСКОЙ КАРТЫ;
* НЕ ОСУЩЕСТВЛЯЙТЕ ПОКУПКИ В СЕТИ ИНТЕРНЕТ НА ПОДОЗРИТЕЛЬНЫХ И НЕЗНАКОМЫХ САЙАХ ПО «ПРИВЛЕКАТЕЛЬНЫМ ЦЕНАМ»;
* ПРЕРВИТЕ РАЗГОВОР, ЕСЛИ ВАМ ЗВОНИТ НЕИЗВЕСТНОЕ ЛИЦО И ГОВОРИТ С ВАМИ О ФИНАНСАХ, ИМЕЮЩИХСЯ БАНКОВСКИХ КАРТАХ;
* НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ;
* НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЕЖНЫЕ СРЕДСТВА НА ЭЛЕКТРОННЫЕ КОШЕЛЬКИ, не убедившись в благонадежности контрагента;
* НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ или МАЛОЗНАКОМЫМ ЛИЦАМ ЛИЧНЫЕ ДАННЫЕ, которые в дальнейшем могут быть использованы Вам во вред.